Technical Disclosure Commons

Defensive Publications Series

December 2020

Secure Sharing of Pre-trained Machine Learning Models For Hands-on Training At Scale

Rui Costa

Casey Palowitch

Secure Sharing of Pre-trained Machine Learning Models For Hands-on Training At Scale

ABSTRACT

This disclosure describes a framework that allows learners to access pre-trained models provided via a public or private computing resource. A model sharing API is described that enables learner applications to make requests that include authentication information, API path, and parameters. The client request is authenticated and a hosted model is run to generate a response which is provided to the learner application via the model sharing API. In this manner, the framework supports providing access to hosted ML models without the learner application having direct access to the models or having control over the computing resources where the model is hosted.

KEYWORDS

- Machine learning
- Data science
- ML model sharing
- ML model access
- Pre-trained model

BACKGROUND

There is a substantial need for individuals with skills in machine learning/ artificial intelligence technology. A major impediment to overcoming the global skills gap in ML/AI is the lack of access to compute resources at scale and the energy required to sustain computations. The training of ever-more-sophisticated multi-parametric machine learning models can take hours to complete. The present teaching methodology of repeated training and re-training of

ML/AI models as individuals learn ML/AI skills is increasingly infeasible. Solutions to this problem are needed to broadly enable the training of ML/AI practitioners.

DESCRIPTION

This disclosure describes a framework that allows learners to access pre-trained models provided via a public or private computing resource. A model sharing API is described that enables learner applications to make requests that include authentication information, API path, and parameters. The client request is authenticated and a hosted model is run to generate a response which is provided to the learner application via the model sharing API. In this manner, the framework supports providing access to hosted ML models without the learner application having direct access to the models or having control over the computing resources where the model is hosted. Fig 1 illustrates the conceptual framework of the system for secure sharing of pre-trained ML models.

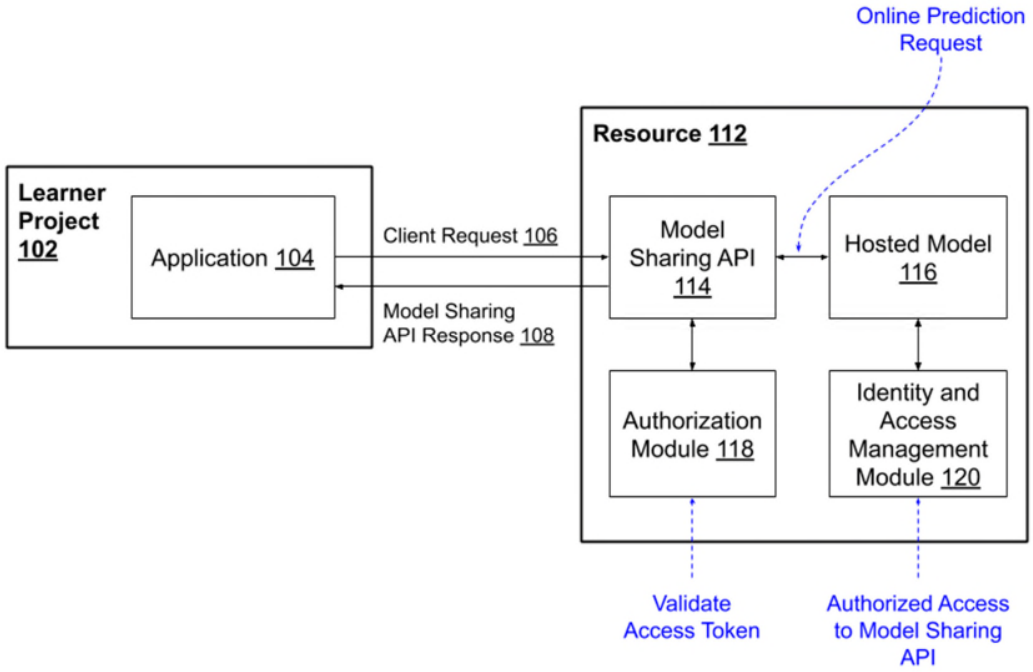

Fig. 1: Framework for securely sharing pre-trained ML models

As seen in Fig. 1, a learner is building or using an application (104) as part of a learner project (102). The application requires access to a machine learning model. An online resource (112) stores hosted model (116) which can include pre-trained models. Access to the hosted model is provided via a model sharing API (114). An authorization module (118) and an identity and access management module (120) are provided and control access to the hosted model. The learner application can make requests to the hosted model via the model sharing API, and if successfully authenticated, receive responses generated by the hosted model.

Components of the framework are described in further detail below.

1. **Application (104):** The application is a learner service that requests access to machine learning models for predictions. The application can be built by the learner or can be provided to them. To successfully access a pre-trained model, the application sends a client request (106) to the model sharing API. The request can include parameters such as an access token, the API path, and one or more parameters.
2. **Model Sharing API (114):** The model sharing API provides requesting applications access to the hosted model, without granting them any access controls to the underlying computational resources. Elevated privileges that are necessary to access the hosted model are granted only to the model sharing API. The model sharing API utilizes the authorization module to validate the access token. For client requests that include valid access tokens, an online prediction request is sent to the hosted model.

   The hosted model utilizes the identify and access management module to authorize the access for client requests received via the model sharing API. The hosted model runs the prediction request and responds with the prediction results, which are passed on to the learner application as a model sharing API response (108).

3. **Hosted Model (116):** The hosted model can run any machine learning framework and can be hosted on any supported compute platform including cloud platforms and/or on-premise environments. Access to the hosted model via the model sharing API can be provided via a public or private IP address, such that the learner has no access or visibility to the hosted model. The model sharing API and the hosted model can also support transfer learning. In transfer learning, a model developed for a task is reused as the starting point for a model on a second task, which allows a learner to use already existing learned tasks from an existing dataset and apply that knowledge to a new dataset that is provided by the learner.

The model sharing API together with an access-controlled hosted model as described in this disclosure can be used to provide learners access to pre-trained models at scale and can be used to train data scientists and machine learning practitioners.

CONCLUSION

This disclosure describes a framework that allows learners to access pre-trained models provided via a public or private computing resource. A model sharing API is described that enables learner applications to make requests that include authentication information, API path, and parameters. The client request is authenticated and a hosted model is run to generate a response which is provided to the learner application via the model sharing API. In this manner, the framework supports providing access to hosted ML models without the learner application having direct access to the models or having control over the computing resources where the model is hosted.

REFERENCES

1. Marr, Bernard. “The AI Skills Crisis And How To Close The Gap” 25 Jun 2018. Available online at https://www.forbes.com/sites/bernardmarr/2018/06/25/the-ai-skills-crisis-and-how-to-close-the-gap/#9fe86e031f39
2. Thompson, Neil C., Kristjan Greenewald, Keeheon Lee, and Gabriel F. Manso. "The computational limits of deep learning." *arXiv preprint arXiv:2007.05558* (2020).
3. SEAB AIML Working Group Preliminary Findings. 12 March 2020. Available online at https://www.energy.gov/sites/prod/files/2020/04/f73/SEAB%20AI%20WG%20PRELIMINARY%20FINDINGS_0.pdf